Tunisian Republic

Tunisian Republic Ministry of Higher Education and Scientific Research

University of Sfax

National School of Electronics and Telecommunications
Telecommunications Department

End of year project
- 2nd year Telecommunications engineering –

Author
Mohamed Amine Garrach

Quantum key distribution protocol : BB84 implementation

Supervisor
Mrs. Manel Boujelben

Examiner
Mr.Faouzi Zarai

Promotion : 2021/2022

Acknowledgement

> “
>
> *First and foremost, I’d want to thank my family, especially my parents, for their unwavering support and encouragement; without them, this report would not be possible,*
>
> *In Addition, I would like to express my gratitude and thanks to Mrs. Manel Boujelben, my University supervisor, for all the valuable advice and the information she gave me and for devoting the time to follow-up of this work,*
>
> *Finally, Thanks to everyone in the quantum computing community for generating such great open source and the opportunity to work on a real quantum computer.*
>
> ”

- Mohamed Amine

Abstract

As the world becomes more digitalized, cryptography becomes increasingly important in preventing cyber attacks. Classical cryptographic protocols rely primarily on the mathematical complexity of encoding functions and the shared key, such as the RSA protocol, whose security is based on the fact that factoring a large number is a difficult problem for modern computers. This means that having a lot of computing power can assist you in cracking traditional encryption methods.

In many cases, quantum machines claim to have this kind of power. Factorization of large numbers with Shor's algorithm and quantum machines may be possible in a reasonable amount of time. Aside from that, the main issue is key sharing, or how to securely share the key for the first time in order to validate the encryption.

Two parties interested in communicating with one other devise a procedure that claims significant protection against an eavesdropper by encoding and decoding information in quantum states to produce and distribute a secret key. Quantum key distribution may be accomplished in a variety of methods. The prospect of a third-party assault, as well as the influence of noise, is explored and implemented.
The IBMQuantum Experience platform was utilized for all of the implementations.

Keywords : Quantum Cryptography, Quantum Key Distribution, BB84 protocol, Photon number splitting attack, IBMQuantum Eperience.

Contents

List of Figures

List of Tables

Introduction

context

Instead of using traditional encryption, quantum cryptography (QA) allows the secure exchange of an encryption key over a private channel.Quantum computing is used in the wireless body sensor network to assure the security of information flow. Quantum key distribution (QKD) is a quantum-based secure communication technology. It will produce a shared random secret key that only the persons involved in the communication will be aware of. Using the known private key, messages are encrypted and decoded.[1]

Problem

The distribution of keys is an important issue in cryptography. The issue is about the following: actions: During key generation, another unauthorized entity may copy or sniff the key.

Goals

Alice and Bob want to establish a secret key for subsequent communication via Classical Channel

Settings

Alice and Bob:

1. a secure Lab

2. access to a Quantum Channel (conserves Qubit states)

3. a classical communication channel (public channel, e.g. internet)

Organization of the report

This dissertation is organized into three chapters:

The First chapter **Background** demonstrate a fundamental notion of quantum computing and the tools required in the next chapters.

The Second chapter **Quantum Key Distribution** Illustrate the detailed steps of the BB84 mechanism with some basic principles to understand the phenomenon of the protocol.

The Third chapter **Implementation of BB84 protocols on IBM QX** demonstrate the implementation of the BB84 protocol utilizing Qiskit Circuit locally and on IBM QX devices , and display the final produced key with a graphic interface.

Chapter 1

Backgroud

This Chapter contains:

1.1 Introduction

Cryptography is a technique used to securely communicate between two parties in a public environment where unauthorized users and malicious attackers are present. There are two processes in cryptography, namely encryption and decryption, which take place at the sender and receiver respectively. Encryption is the process of combining simple multimedia data with some additional data (called a key) and converting it into an unreadable encrypted format called a cipher. Decryption is the opposite of encryption, using the same or other additional data (key) to decrypt the password and turn it into real multimedia data.

Cryptographic techniques can be classified according to their rationale or the protocols they follow. But here, we will focus on two types of cryptography: classical cryptography and quantum cryptography.

1.2 Classical Cryptography

1.2.1 Principle of cryptography

Classical cryptography is predicated on the mathematics and it relies on the computational difficulty of factorizing sizable amount . the safety of classical cryptography is predicated on the high complexity of the mathematical problem for the instance factorization of huge number.
In the classical cryptography the first data i.e., the plain text is transformed into the encoded format i.e. cipher text in order that we will transmit this data through insecure communication channels. a knowledge string which referred to as key's wont to control the transformation of the info from plain text to cipher text. This arrangement helps to stay data safe because it required the key for extracting the first information from the cipher text. Without the key nobody can read the info. During this technique it's assumed that the sole authorized receiver has the key.[2]

Classical Cryptography has two types of techniques:

Symmetric Cryptography

A single key is used in symmetric key cryptography to encode and decode data. This encryption key is a personal key. This encryption technique's restriction is that the private key may only be communicated to the authorized sender and receiver.[2]

Asymmetric Cryptography

Asymmetric cryptography uses a two different keys, namely a public key and a private key, for encryption and decryption. A sender can encrypt data with its public key, while the receiver can decrypt it using its private key. This approach solves the problem of key distribution.[2]

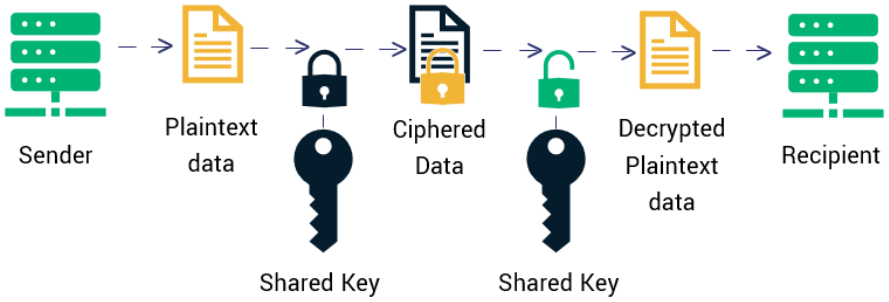


Figure 1.1: Symmetric-encryption

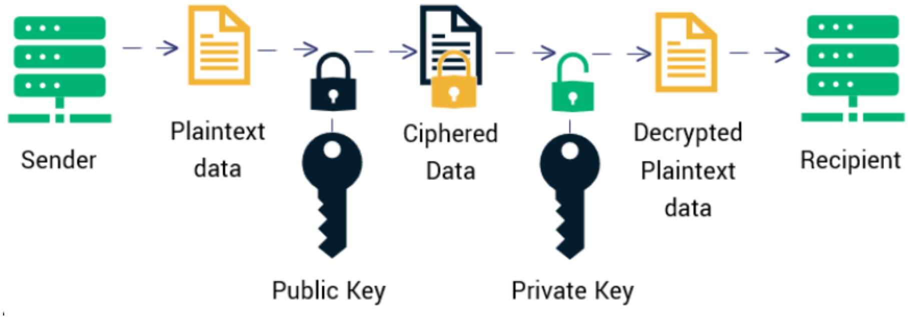


Figure 1.2: Asymmetric-encryption

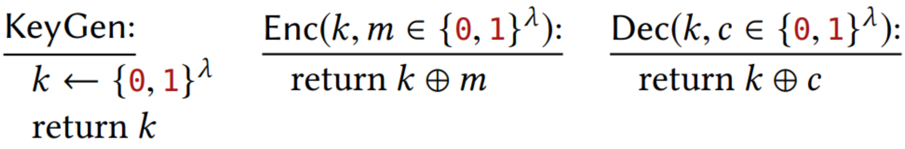
1.2.2 One-time-pad and key distribution problem

People have been attempting to convey secret communications for around 2000 years, but only two viable concepts from before 1900 have any relevance to current cryptography. The concept is one-time pad (OTP), which demonstrates numerous key ideas and may still be found deep inside many current encryption systems.

The technique is sometimes referred to as ”Vernam’s cipher” after Gilbert Vernam, a telegraph engineer who invented it in 1919. However, an older explanation of one-time pad was recently uncovered in an 1882 essay on telegraph encryption by Frank Miller.

Secret keys will be strings of bits in the majority of this report. We normally utilize the variable to inquire the length (of bits) of the key, such that keys are elements of the set $\{0, 1\}^\lambda$. In the case of a one-time pad, the choice of λ has no effect on security ($\lambda = 10$ is ”just as secure” as $\lambda = 1000$); nonetheless, the key and plaintext lengths must be compatible.

Not only are the keys λ-bit strings present in one-time pad, but so are plaintexts and ciphertexts. Consider this a simple coincidence, because we’ll soon meet schemes in which the keys, plaintexts, and ciphertexts are all strings of varying lengths.[3]



```
KeyGen:
    $k \leftarrow \{0, 1\}^\lambda$
    return $k$

Enc($k, m \in \{0, 1\}^\lambda$):
    return $k \oplus m$

Dec($k, c \in \{0, 1\}^\lambda$):
    return $k \oplus c$
```

Figure 1.3: One-time pad

Recall that “k $\leftarrow \{0, 1\}^\lambda$” means to sample k uniformly from the set of λ -bit strings.

This uniform choice of key is the only randomness in all of the one-time pad algorithms. As we will see, all of its security stems from this choice of using the uniform distribution; keys that are chosen differently do not provide equivalent security.

Even a quantum computer cannot hack one-time-pad (OTP) encryption. The necessity to securely share supplies of symmetric random keys rendered the technology nearly useless as a stand-alone solution for quick and high-volume telecommunication. Essentially, this secure key exchange and renewal had to be done via couriers, which was a long and costly process.[3]

1.3 Essential Quantum principles utilized

1.3.1 What is a Qubit ?

A qubit (or quantum bit) is the quantum mechanical equivalent of a bit. In traditional computing, information is represented in bits, with each bit having a value of zero or one. Information in quantum computing is encoded in qubits. A qubit is a two-level quantum state with the two base qubit states represented as $|0\rangle$ and $|1\rangle$. A qubit can bin the states $|0\rangle$, $|1\rangle$, or (unlike a traditional bit) a linear mixture of both.[4]

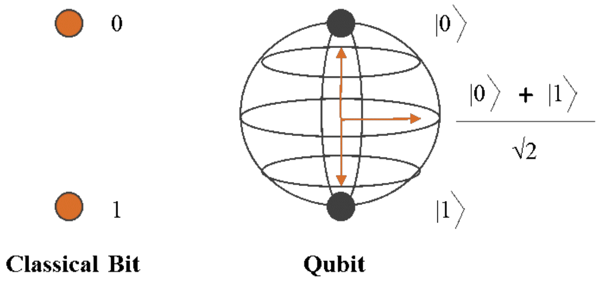


Figure 1.4: Qubit and bit

1.3.2 Quantum Gate

We saw that qubits could be represented by 2D vectors, and that their states are limited to the form: $|q\rangle = \cos\frac{\theta}{2}|0\rangle + \exp i\phi \sin\frac{\theta}{2}|1\rangle$
Where θ and ϕ are real numbers. This section will go over gates, which are the operations that switch a qubit between these states.[5]

The Pauli Gate

The Pauli-X gate is the quantum equivalent of the NOT gate for classical computers with respect to the standard basis $|0\rangle$,$|1\rangle$.[5]

The X-gate is represented by the Pauli-X matrix: X = $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Similarly to the X-gate, the Y & Z Pauli matrices also act as the Y and Z-gates in the quantum circuits: Y= $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ Z= $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Hadamard Gate [4]

The Hadamard gate is a single-qubit operation that maps the basis state $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$,thus creating an equal superposition of the two basis states. H=$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

T and S Gate [5]

The T gate is a single-qubit operation given by: T= $\begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{i\pi}{4}\right) \end{pmatrix}$
The T gate is related to the S gate by the relationship $S = T^2$
The conjugate transpose of the T gate is defined by: $T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{-i\pi}{4}\right) \end{pmatrix}$

1.3.3 Measurement

For the measurement of a qubit, there are two potential outcomes: ”0” and ”1,” much like a bit or binary digit. However, unlike a bit, which can only be either 0 or 1, the general state of a qubit can be a coherent superposition of both according to quantum physics. Furthermore, although measuring a conventional bit does not damage its state, measuring a qubit destroys its coherence and irreversibly disturbs the superposition state. One bit can be entirely encoded in one qubit.

Quantum measurement is an irreversible procedure that gains information about the state of a single qubit while losing coherence. The result of the measurement of a single qubit with the state $\psi = \alpha|0\rangle + \beta|1\rangle$ will be either $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$.
Measurement of the state of the qubit alters the magnitudes of α and β. For instance, if the result of the measurement is $|1\rangle$, α is changed to 0 and β is changed to the phase factor $e^{i\phi}$ no longer experimentally accessible. [6]

1.3.4 Heisenberg’s Uncertainty Principle

This principle asserts that only one characteristic of a pair of conjugate properties, such as location and momentum, may be known with confidence in a quantum state (a reasonable measurement of a particle’s position will upset its momentum). Quantum cryptography takes use of this by using the conjugate features of photon polarization (as photons may be transferred across fiber optic networks) on distinct bases.[7]

1.3.5 No-Cloning Theorem

We rely largely on the capacity to copy in traditional computers. Even the most basic classical operation, addition, is based on bit copying. It is, however, impossible with quantum computing.

We simply cannot use the information stored in a qubit as many times as we would like in quantum computing. In reality, duplicating a qubit in an arbitrary state would violate the fundamental concept of superposition. Measuring a qubit causes its state of superposition to collapse. However, if we could clone a qubit, we could indirectly measure its state. We were able to measure the clones without having to collapse the original qubit.[8]

1.3.6 Quantum Entanglement

Regardless of distance, two quantum particles can entangle in such a way that when one particle's property is measured, a correlated state of the property appears on the other particle. Entanglement is used in quantum teleportation to communicate via a traditional information channel.[7]

Chapter 2

Quantum Key Distribution

This Chapter contains:

2.1 Principle

On this chapter show a general principal and a typical system of Quantum Key Distribution (QKD).
Figure 2.1 depicts a typical QKD setup. Two partners, commonly known as Alice and Bob, want to establish a secret key at a distance. They must be linked by two channels: a quantum channel that allows them to communicate quantum signals, and a classical channel that must be validated (i.e Alice and Bob must certifiably identify themselves). A third person, on the other hand, can observe but not engage in the dialogue. The quantum channel, on the other hand, is vulnerable to third-party manipulation. The objective of Alice and Bob is to provide security against an antagonistic eavesdropper, generally referred to as Eve, who taps into the quantum channel and listening in on the classical channel. [9, 10]

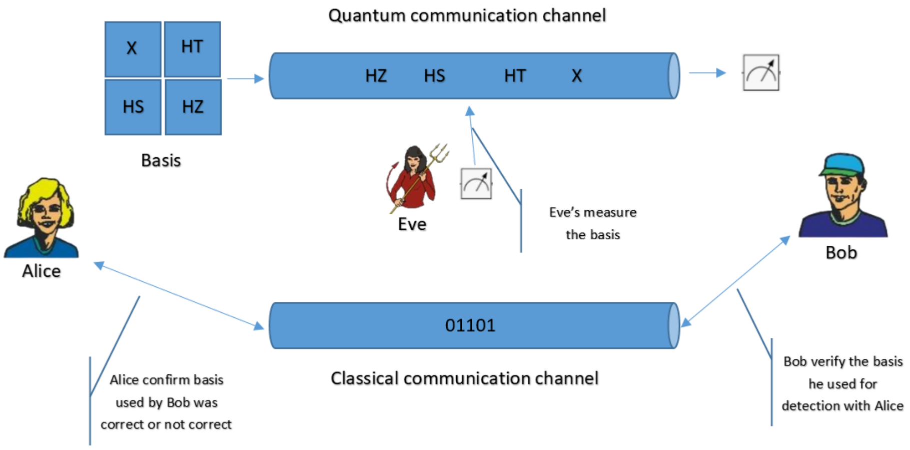

Quantum communication channel
X
HT
HS
HZ
Basis
HZ HS HT X
Eve
Eve's measure the basis
Alice
Bob
01101
Classical communication channel
Alice confirm basis used by Bob was correct or not correct
Bob verify the basis he used for detection with Alice

Figure 2.1: A diagram of a QKD system in which Alice and Bob are linked by a quantum channel, into which Eve can tap without restriction other than the principles of physics, and an authorized classical channel, into which Eve can only listen.

2.2 BB84 protocol

In the BB84 protocol, Alice can transmit a random secret key to Bob by sending a string of photons (Qbits) with the secret key is encoded in their polarization (Encoded basis). The no-cloning theorem guarantees that Eve cannot measure these photons and transmit them to Bob without disturbing the photon's state in a detectable way. The above is true, considering no error on the quantum channel. If the channel is prone to error, Alice and Bob will not detect Eve's presence all the time.[7]

Remark: In this rapport we will use a different basis described in the chapter 1, So we have Four basis to work with HT, HS, HZ, X .

Table 2.1: Coding scheme for the BB84 protocol.

bit	**X**	**HT**	**HS**	**HZ**
0	a_{000}	a_{010}	a_{100}	a_{110}
1	a_{001}	a_{011}	a_{101}	a_{111}

The BB84 can be described as follows [11]:

1. Quantum Transmissions (First Phase)
   - (a) Alice chooses a random string of bits $d_n \in$ {0,1} , and a random string of encoding bases $b_n \in$ {H, HT, HS, HZ}^{n} , where n > N .
   - (b) Alice prepares a photon in quantum state a_{ijk} for each bit d_i in d and b_i in b , and sends it to Bob over the quantum channel.
   - (c) With respect to either basis chosen at random, Bob measures each a_{ijk} received. Bob's measurements produce a string $d_n^{'}$ ∈{0,1} , while his choices of decoding bases form $b_n^{'} \in$ {H, $T^{\dagger}$H, $S^{\dagger}$H, ZH}^{n} .
2. Public Discussion (Second Phase)
   - (a) For each bit d_i in d
     - i. Alice delivers the value of bi to Bob via the classical channel.
     - ii. Bob answers to Alice by stating if he utilized the same measuring foundation. If b_n ≠b$_n^{'}$, both d_i and $d_n^{'}$ are eliminated.
   - (b) Alice selects a random selection of the remaining bits in d and communicates their values to Bob via the channel (over internet for example). Eavesdropping is discovered and communication is terminated if the results of Bob's measurements for any of these bits do not match the values given.
   - (c) The common secret key is the string of bits that remains in d after the bits revealed in step 2b) are deleted, K = {0,1}^{N} .

To detect Eve, Alice and Bob do an eavesdropping test in step 2b) of the protocol. Wherever Alice and Bob's bases are equal (i.e. $b_n = b_n^{'}$), the corresponding bits should be same (i.e. $d_n = d_n^{'}$). If an external disruption occurs or there is noise in the quantum channel, we assume Eve is to blame.

2.3 Classical Authenticated Channel

In a standard person-in-the-middle scenario, we have Eve sitting in between Alice and Bob, executing BB84 with both of them simultaneously. Alice and Bob, to authenticate one another, make contact out of band, by contacting the other on a physically and logically separate channel that Eve has not intercepted. In that sense, we augment the usual picture of BB84 by another channel, shown dashed in Figure 2.1.

Let us return to an essential assumption that is generally made while discussing the BB'84 protocol: that the communication channel between Alice and Bob, dubbed the "CAC," is exactly what its name implies: an authenticated channel. This assumption is intended to ensure that, while the eavesdropper can intercept any conversation, she cannot "impersonate" Alice or Bob by passing bogus messages through the channel. You can easily imagine the disastrous consequences of such an attack: for example, Eve could lie to Bob about Alice's choice of the test set T, thereby increasing its size; Bob would then reveal his results in the larger set, and Eve could keep them as additional side information about Alice's raw key.This assumption is usually considered "benign", as indeed the access to an authenticated channel is a prerequisite for a large variety of cryptographic tasks. Thus in practice one imagines that any two parties Alice and Bob wanting to implement QKD have access to such a channel, that has been implemented by other means. It is still interesting to consider how reasonable the assumption is, and how an authentication channel can be constructed. There are two main methods to achieve authentication, and each has its drawbacks. The first is to use public-key cryptography, which requires computational assumptions on the power of the eavesdropper. The second is to use private-key cryptography, which requires Alice and Bob to share a secret key... [12]

2.4 Attacks on BB84 protocol

Although the ideal description of the BB84 protocol stated above ensures that it is unbreakable, it is virtually impossible to execute the theory completely in real life. Due to flaws in both the generation and measurement of photons, there are several ways to execute quantum hacks, breaking quantum key distributions by exploiting flaws in the implemented system. The following are some eavesdropping techniques.[13]

2.4.1 Intercept-Resend strategy

Intercept-Resend is a less complex eavesdropping approach. In this approach, Eve acts like a normal individual, detecting photons from the Alice side in the same way that Bob does. She would intercept Alice's sent data and measure it using his own established foundation. She would prepare a new state in the measured polarization based on the results of her measurement and transmit it to Bob.

2.4.2 Photon Number Splitting Attack

Lutkenhaus and colleagues discovered in the year 2000 that the existence of multi-photon pulses has a significant impact on the security of the BB84 protocol [14]. They described an assault known as the photon-number splitting attack:

1. Eve keeps track of the amount of photons.
2. If the pulse contains more than one photon, she stores one in a quantum memory and sends the others across a lossless channel.
3. When the foundation is disclosed, she measures the photon she has saved and receives all of the knowledge.

The sole limitation Eve is required to follow is that the raw detection rate on Bob's side not decline. It should be noted that Eve does not create any errors with this assault.[15]

2.4.3 Intermediate basis method

In this way, Eve measures photons using an intermediate basis rather than the same bases that Alice and Bob use. Eve now has probabilistic information. This is a probabilistic eavesdropping method.

It should be noted that we cannot separate mistakes caused by noise from errors caused by eavesdropping activity in theory. As a result, we presume that all mistakes are the result of eavesdropping.

2.5 Conclusion

Quantum cryptography is the technique of using quantum principles to encode information on quantum carriers and securely distribute the cryptographic key between sender and receiver. Bennett and Brassard's original QKD approach, BB84, encodes key bits by using the polarization state of single photons. In an ideal environment, BB84 is impenetrable to all attackers, due to the random nature of individual quantum occurrences.

In the next chapter, we'll look at how to develop the BB84 protocol using a local and real-world device simulator and compare the outcomes with and without Eve attacks on the connection.

Chapter 3

Implementation of BB84 protocol on IBM QX

This Chapter contains:

3.1 Objective

This chapter will discuss the implementation of BB84 protocols on the IBM QX. Assume Alice wishes to share a secret key with Bob over this protocol. First, Alice selects an even binary number. Then, when delivering the data to Bob, Alice encodes her data using four distinct bases. For each of the four bases, Alice selects a unitary gate at random from which Bob may decode the data using the reciprocal corresponding to each gate utilized. The four bases utilized are X, HT (Hadamard gate and T gate applied sequentially), HS (Hadamard gate and S gate applied consecutively), and HZ (Hadamard gate and Z gate applied consecutively). Finally, Bob decrepits the data at random by utilizing the reciprocal of the bases and measures the descripted data.In this scenario, the next section describes the implementation method.

3.2 BB84 protocol: Simulation and Results without Eve

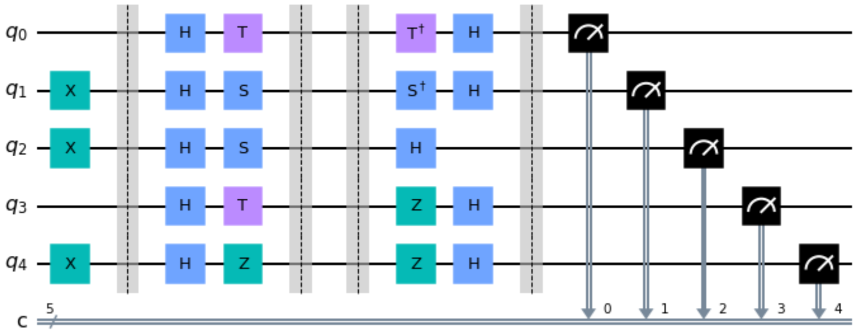


Figure 3.1: Implementation BB84 protocol with Qiskit circuit.

This Circuit describes five distinct parties. First, before the first left barrier, Alice initializes her bit-string, which in this circuit equals 01101. Second, between the first and second barriers, Alice wishes to encode her bit-string using encoding bases chosen at random. Third, between the second and third barriers, this section describes the quantum channel over which Alice and Bob wish to exchange quantum data (qubits). Fourth, between the third and fourth barriers, Bob receives the data and randomly decodes it. Fifth, Bob's measures are located on the right side of the fourth barrier.

TABLE 1: The initial bit-string is produced by five qubits, two of which are left as default with no alteration, such as q[0] and q[3], but q[1], q[2], and q[4] are changed from |0> to |1> by utilizing the X gate. To share the key between Alice and Bob, they must have the same basis as shown in the table.
Alice should encode the data using a random selection of bases, as shown in Table 1, but Bob should decode each qubit using the reciprocal of the bases chosen by Alice.

Table 3.1: 5-Qubits Random Values by Alice and Bob

Qubit	**q[0]**	**q[1]**	**q[2]**	**q[3]**	**q[4]**
Initial Bit-string's gate construction	-	X	X	-	X
Initial bit-string	0	1	1	0	1
Alice's gates for string encoding	HT	HS	HS	HT	HZ
Bob's gates for string decoding	$T^{\dagger}$H	$S^{\dagger}$H	H	ZH	ZH
Alice's Basis	HT	HS	HS	HT	HZ
Bob's Basis	HT	HS	H	HZ	HZ
Result	√	√	x	x	√

For example, Alice may select $T^{\dagger}$H to encode the first qubit, whereas Bob may select TH to decode the qubit. In this situation, we should use Hamiltonian gates, i.e. $TT^{\dagger}$=I, and the same goes for the S gate.

3.2.1 Simulation using local simulator

In this section, we'll use 5 Qubits as an example, but first, let's look at the various outcomes that may be predicted based on the chance of receiving that specific bit after measurement.

Table 3.2: Output result expected

Qubit	**Expected Result**
q[0]	0 (100%)
q[1]	1 (100%)
q[2]	0 (50%) & 1 (50%)
q[3]	0 (50%) & 1 (50%)
q[4]	1 (50%)

This local simulator is intended for quick prototyping and testing in classical machines in order to approximate quantum calculations. We note that the predicted outcome in Table 3.2 is the same in the implementation.

3.2.2 Simulation using real quantum device(ibmq manila)

Because of the error calculation, the implementation of the BB84 protocol using an actual quantum device yields different results in this section. Using an 8192-run ibmq manila as

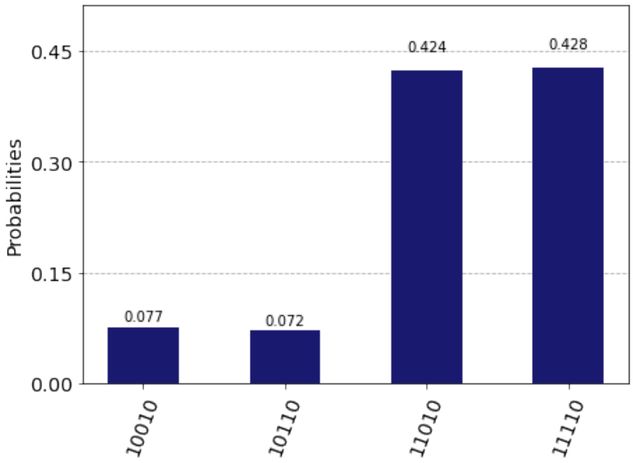


Figure 3.2: Implementation BB84 protocol using local simulator.

a quantum gadget, Figure 3.3 show the results of the implementation.

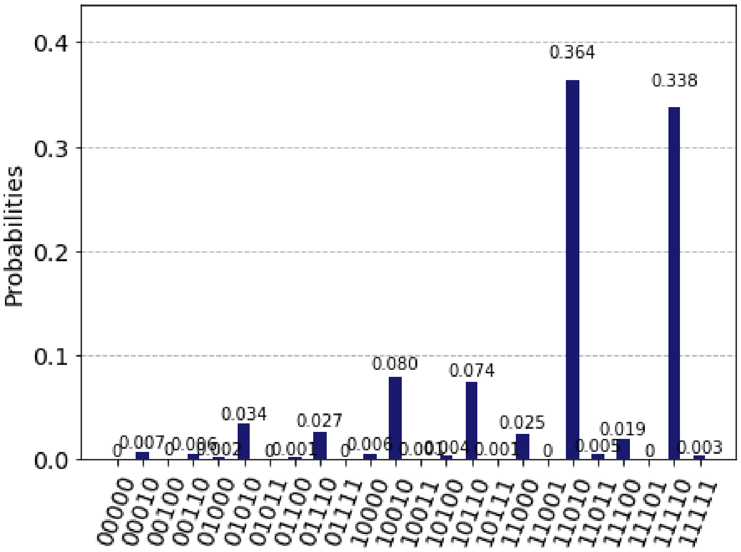


Figure 3.3: Implementation BB84 protocol using IBMQ manila.

After measuring all of the qubits, we can see that it has more outputs in Figure 3.3 than the local implementation in Figure 3.2, but with different probabilities, for example, q[1] is not 1, implying that the likelihood of gaining 1 is less than predicted 100%. The same is true for the other qubits.

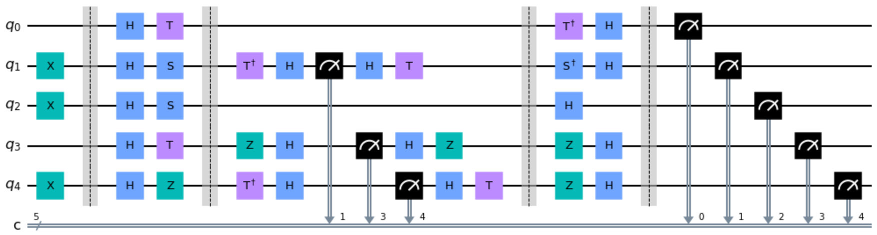


Figure 3.4: Eavesdropper Attacks on the Quantum Circuit.

3.3 BB84 protocol: Simulation and Results with Eve

3.3.1 Simulation using local simulator

This section interprets the third half of the quantum circuit, which is located between the second and third barriers. That eavesdropper targeted the quantum channel, namely the second, fourth, and fifth qubits. The foundation for decrypting Alice's encryption bit-string provided to Bob is chosen at random by the eavesdropper, who then measures the decrypted qubits. We are discussing the no cloning theorem, which states that Eve cannot measure the qubits without changing the information scanned. So Eve encrypts the bits he hacked on a random basis and sends them to Bob.
Figure 3.6 depicts the outcome of the BB84 implementation when subjected to the Eavesdropper attack.

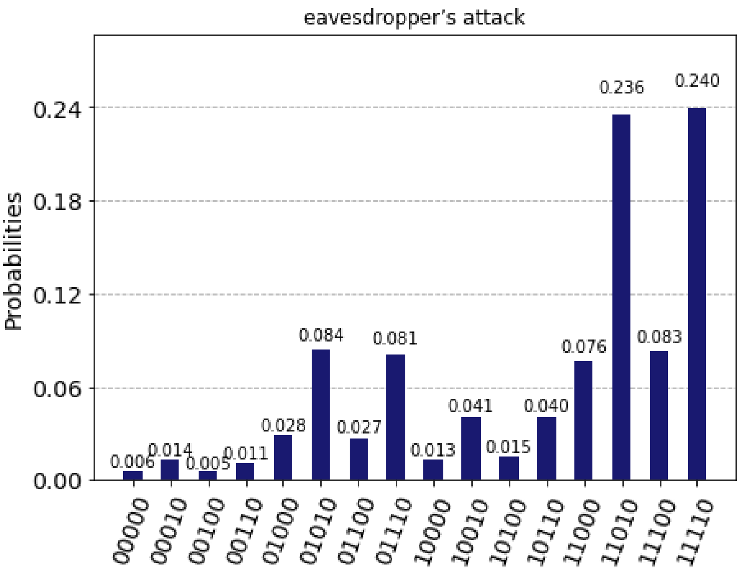


Figure 3.5: Eavesdropper Attacks on local simulator.

We see that when an eavesdropper intercepts the circuit, the outcome of the implementation changes, causing the probabilities and number of qubits to appear to alter. However, the last bit-string has the highest probability in the final findings. That is, in this scenario, Eve's attack has no effect on the outcome. Alice and Bob can securely trade their secret key.

3.3.2 Simulation using real quantum device(ibmq manila)

In this section, the implementation of the BB84 protocol using a genuine quantum device yields different outcomes due to error computation and man-in-the-middle attacks. Figure 3.5 depicts the implementation results using ibmq manila as a quantum device and 8192 runs. Figure 3.5 show the results of the implementation.

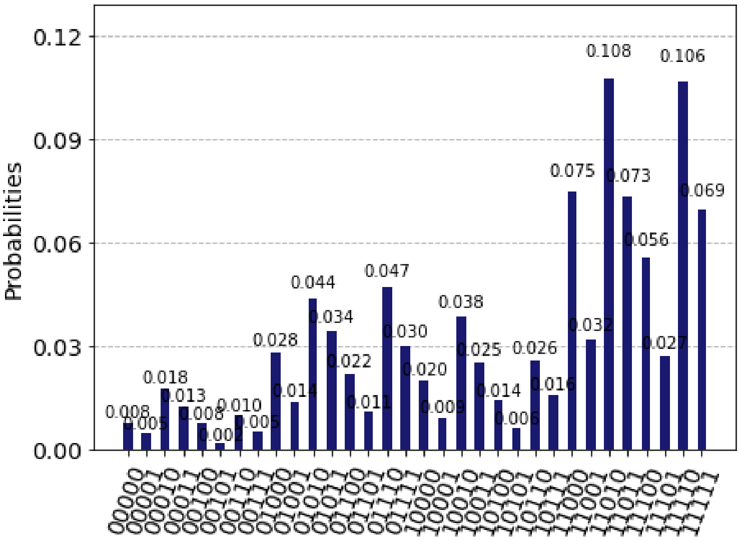


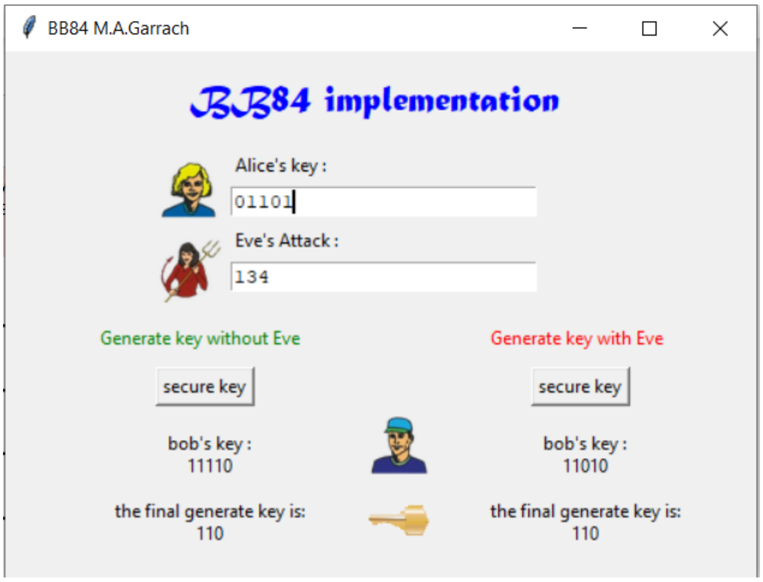
Figure 3.6: Eavesdropper Attacks on IBMQ manila.

Results for an eavesdropper's attack on the BB84 protocol using 5 qubits on IBM QX (ibmq manila). Eve measures q[1], q[3], and q[4]. She correctly answers q[3]. Once Bob has provided his measures to you, they will be revealed. If they were Alice, they would notice the eavesdropping.[16]

3.4 BB84 Graphic User Interface (GUI)

This section demonstrates the practical use of the BB84 protocol by taking an Alice's key (bit-string) and Eve's attacks (a string describing each number in this string presented the qubit index that Eve attacked) as inputs and producing two bit-strings as outputs, one for the bob's key bit-string and the other for the final generating key for Alice and Bob to use.

Figure 3.7 depicts two distinct parties. The first is the left half, in which we may produce a secret key without the help of an Eavesdropper, and the second is the right part. those codes describe the two different parties and the mechanism of the implementation.



BB84 M.A.Garrach

BB84 implementation

Alice's key :
01101

Eve's Attack :
134

Generate key without Eve

secure key

bob's key :
11110

the final generate key is:
110

Generate key with Eve

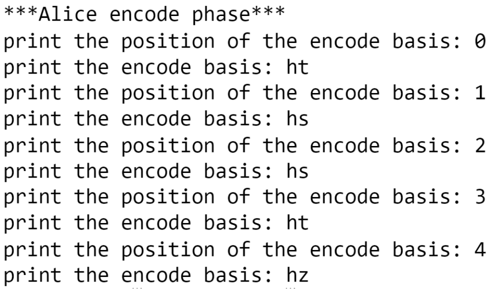
secure key

bob's key :
11010

the final generate key is:
110

Figure 3.7: BB84 Graphic User Interface

Now we'll look at how the interface's implementation works. First, enter the string-bit in both the Alice's key box and the Eve's Attacks box.As seen in Figure3.8, Alice coded her data on a random basis. Second, Eve intercepts the quantum channel and must decode, measure, and code the data. Figure3.10 depicts the basis Eve utilized to decrypt and subsequently encrypt Alice's encoding data. Finally, Bob should decrypt the encrypted data using a randomly generated decoding base, as shown in Figure3.11.



```
***Alice encode phase***
print the position of the encode basis: 0
print the encode basis: ht
print the position of the encode basis: 1
print the encode basis: hs
print the position of the encode basis: 2
print the encode basis: hs
print the position of the encode basis: 3
print the encode basis: ht
print the position of the encode basis: 4
print the encode basis: hz
```

Figure 3.8:
Randomly encoding Alice's Basis

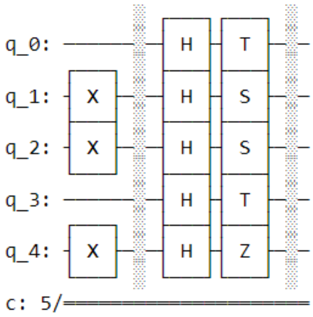
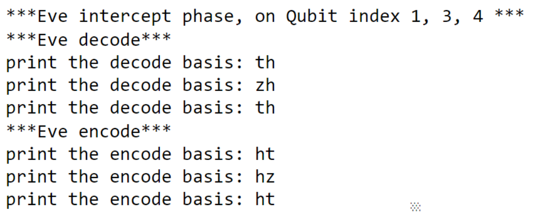


Figure 3.9:
Alice's encoding circuit

Figure3.9 depicts Alice's encoding circuit, which she created by selecting the following foundation in Figure3.8. That Alice encode all of the bits that were initialized before to the encoding operation.



```
***Eve intercept phase, on Qubit index 1, 3, 4 ***
***Eve decode***
print the decode basis: th
print the decode basis: zh
print the decode basis: th
***Eve encode***
print the encode basis: ht
print the encode basis: hz
print the encode basis: ht
```

Figure 3.10:
Randomly decoding/encoding Eve's Basis

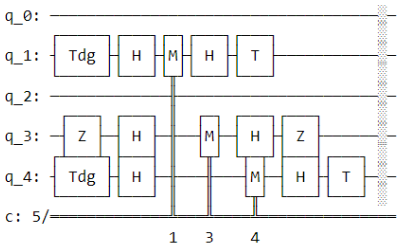
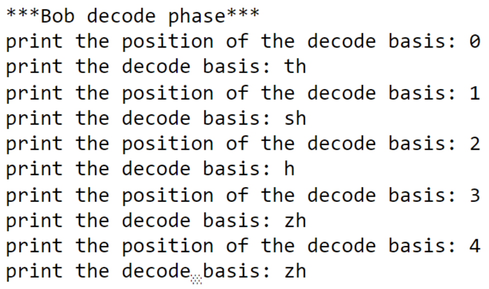


Figure 3.11: Eve's intercepting circuit

Figure3.11 depicts a circuit that Eve intercepts in the quantum channel, which is made up of three parts: decoding, measuring, and decoding, and which Eve created by selecting the following basis in Figure3.10. That Alice encode all of the bits that were initialized before to the encoding operation.



```
***Bob decode phase***
print the position of the decode basis: 0
print the decode basis: th
print the position of the decode basis: 1
print the decode basis: sh
print the position of the decode basis: 2
print the decode basis: h
print the position of the decode basis: 3
print the decode basis: zh
print the position of the decode basis: 4
print the decode basis: zh
```

Figure 3.12: Randomly decoding Bob's Basis

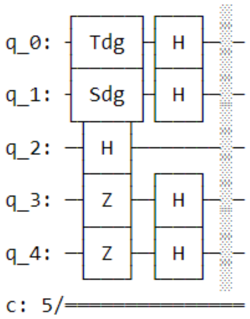


Figure 3.13:
Bob's encoding circuit

Figure3.13 depicts Bob's decoding circuit, which he created by selecting the following foundation in Figure3.12. That Bob decode all of the encoded Qubits and measure them in the last phase to obtain "Alice's bit-string."

3.5 Conclusion

Finally, the local simulation in the quantum circuit yields the desired outcome. The implementation using a real quantum device, on the other hand, yields different results with a probability less than the probability of the local simulation; this variability in probability and the inspected result is due to differences between these systems, which are represented by the number of qubits, their connectivity, and the system error rates.

Conclusion

Quantum cryptography might potentially be used to provide completely and provably secure communication in which the adversary cannot decipher the transmission regardless of the amount of processing power and time available. However, the technology is still in its early stages and is developing. As academics learn more about this and conduct further study, they discover errors in some of their prior assumptions and results. Given its limitations, it is difficult to envisage this technology being used in practice today. However, with future advances in quantum transmission, computation, and cryptography, it may just present us with a truly secure communication means.

Bibliography

[1] **quantum key distribution (QKD)**. Alexander S. Gillis : https://www.st.com/content/st_com/en/about/st_company_information/who-we-are.html

[2] **Classical Cryptography and Quantum Cryptography**. 08 Aug, 2019 : https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography

[3] **Untappable key distribution system: a one-time-pad booster**. Geraldo A. Barbosa and Jeroen van de Graaf : https://arxiv.org/pdf/1406.1543.pdf

[4] **What is a qubit?**. Quantum Inspire by Quteck: https://www.quantum-inspire.com/kbase/what-is-a-qubit/

[5] **Single Qubit Gates**. Learn Quantum Computation using Qiskit by IBMQuantum: https://qiskit.org/textbook/ch-states/single-qubit-gates.html

[6] **Single Qubit Gates**. Learn Quantum Computation using Qiskit by IBMQuantum: https://qiskit.org/textbook/ch-states/single-qubit-gates.

[7] **Quantum Key Distribution and BB84 Protocol**. MR.Asif Jun 24, 2021: https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5

[8] **Quantum Computing Is Different, The No-Cloning Theorem**. Frank Zickert | Quantum Machine Learning Dec 1, 2020: https://towardsdatascience.com/quantum-computing-is-different-2178fba922cd

[9] **“The security of practical quantum key distribution”**. V. Scarani, H.Bechmann- Pasquinucci, N.J. Cerf, N. Lütkenhaus, M. Peev, Reviews of modern physics vol. 81, pp. 1301-1310,2009

[10] **“Quantum Cryptography”**. N. Gisin, G. Ribordy, W. Tittel, and H. Zbiden, Rev. Mod. Phys., vol. 74, pp. 145-195, 2002.

[11] **“Implementation of secure key distribution based on quantum cryptography”**. M. Elboukhari, M. Azizi, A. Azizi, in Proc. IEEE Int. Conf Multimedia Computing and Systems(ICMCS’09), page 361 - 365, 2009.

[12] Nelly Ng Stephanie Wehner. Week 0. In edX Quantum Cryptography. 2018. Lecture Notes.

[13] **“Study of BB84 QKD protocol: Modifications and attacks”**. Priyanka M.,Sandra K¨onig, Dr. Urbasi Sinha :
http://reports.ias.ac.in/report/18088/study-of-bb84-qkd-protocol-modifications-and-attacks

[14] Heinrich M. Jaeger, Sidney R. Nagel, and Robert P. Behringer. Granular solids,liquids, and gases. Rev. Mod. Phys., 68:1259–1273, Oct 1996.

[15] Valerio Scarani, Antonio Ac´ın, Gr´egoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters, 92(5), Feb 2004.

[16] **“Experimental realization of BB84 protocol with different phase gates and SARG04 protocol”**. Sinchan Ghosh,1, ∗Harsh Mishra,2, †Bikash K. Behera,3, ‡and Prasanta K. Panigrahi4, September 2021.